Verfahren zur Übertragung von Informationen über IP-Netzwerke

Beschreibung

Die Erfindung betrifft ein Verfahren zur Übertragung von Informationen über IP-Netzwerke. Insbesondere ein Verfahren zur Übertragung von Informationen durch mobile Endgeräte, wie mobile Telefone oder PDAs, die unter anderem einen Zugang zu herkömmlichen Funknetzwerken wie GSM oder UMTS besitzen. Sollten diese Geräte in einem reinen IP basierten Netzwerk arbeiten, wie UMTS oder Wireless LAN, so ist es sinnvoll, bestehende Standards aufzugreifen, um einerseits einen einfachen Übergang zu vorhanden Technologien zu erreichen und andererseits dem Benutzer eine leichte Anwendung zu ermöglichen.

GPRS für GSM und UMTS ermöglichen ein paketorientiertes Netzwerk auf der Basis von UMTS und GSM auf der letzten Meile. Die Vorteile der so genannten paketorientierten Domänen ist ihre Kompatibilität untereinander sowie mit dem Internet. So gibt es eine Reihe von Anwendungen, die speziell für IP basierte Netzwerke entwickelt wurden. Aus diesem Ansatz heraus ergibt sich, dass GPRS ein sehr wichtiger Bestandteil von neuen UMTS Netzwerken sein wird. Aufgrund der Beschränkungen von UMTS in sehr stark frequentierten Bereichen wie z. B. in der Umgebung eines Unternehmens oder einer Universität wird UMTS nicht allen Ansprüchen gerecht werden. So wird es für einen Provider nahezu unmöglich sein, alle Aufgaben mit einem

UMTS-GSM Netzwerk zu lösen. In solchen Bereichen wird z. B. Wireless LAN (IEEE802.11(x), ETSI Hiperlan) Einzug halten um die UMTS Infrastruktur zu entlasten. In einer solchen gemischten Architektur ist es wichtig, dass eine Kommunikation zwischen den unterschiedlichen Domänen möglich ist.

Aufgabe der Erfindung ist es, ein Verfahren und eine Vorrichtung bereitzustellen, die eine Interoperabilität erlauben, unabhängig davon, in welchem Typ von Netzwerk sich der mobile Benutzer befindet.

Diese Aufgabe wird durch die Erfindungen gemäß den Merkmalen der unabhängigen Ansprüche gelöst. Vorteilhafte Weiterbildungen der Erfindungen sind in den Unteransprüchen gekennzeichnet.

Abstrakt betrachtet besteht die Erfindung aus 2 Komponenten. Die eine Komponente ist auf dem mobilen Endgerät angeordnet, wobei Informationen dem GPRS-Standard entsprechend in IP-Pakete gebettet werden, um sie durch einen IP-Tunnel zu dem zweiten Bestandteil der Erfindung zu übermitteln. Bei diesem zweiten Bestandteil handelt es sich um einen IP Serving GPRS Support Node (IP-SGSN) im IP-Netzwerk, der die Pakete aus dem Tunnel empfängt und sie entpackt, um sie dann z. B. an einen weiteren GSN zu schicken, der wiederum verantwortlich für andere mobile Endgeräte ist oder über den eine Verbindung mit dem Internet ermöglicht wird (GGSN). Die zweite Komponente hat somit für weitere GSN nach außen die Form eines herkömmlichen SGSN, wobei sie in Richtung des mobilen Endgerätes als Ende eines Tunnels zu betrachten ist. Beim Tunneln von Informationen werden Pakete eines anderen Protokolls in ein IP Paket eingepackt, sodass im Datenbereich des IP-Paketes ein vollständiges, in diesem Falle GPRS-, Paket anzutreffen ist.

Im Einzelnen handelt es sich um ein Verfahren zur Übertragung von Informationen mittels GPRS in einem IP-Netzwerk, insbesondere einem Wireless LAN und/oder einem Hiperlan-

Netzwerk, mit einem vorzugsweise mobilen Endgerät, das mit dem IP-Netzwerk in Verbindung steht, so dass IP-Pakete ausgetauscht werden können. Ein weiterer Bestandteil der Erfindung ist ein IP Serving GPRS Support Node im IP-Netzwerk, wobei beim Initialisieren der Verbindung zwischen dem Endgerät und dem IP Serving GPRS Support Node ein Tunnel auf der Basis von IP-Paketen aufgebaut wird, der GPRS-Informationen tunnelt. Die Übertragung von Informationen erfolgt im Folgenden durch den Tunnel. Der IP Serving GPRS Support Node ist über ein IP-Netzwerk mit weiteren Serving GPRS Support Nodes, Gateway GPRS Support Nodes sowie anderen GPRS Service Nodes (z. B. für SMS) verbunden, wobei der IP SGSN die Informationen je nach Richtung der Kommunikation auspackt und/oder umpackt, um die Informationen den weiteren GPRS Service Nodes zu senden, oder einpackt, um die Informationen durch den Tunnel zum Endgerät zu senden.

Aufgrund der Besonderheit dieses Verfahrens muss auf herkömmlichen mobilen Endgeräten eine weitere Software installiert werden, die für den Benutzer transparent das Ein- und Auspacken von Informationen übernimmt. Weiterhin ist diese Software so ausgebildet, dass sie versucht, einen IP SGSN zu finden, sobald sie Kontakt zu einem IP-Netzwerk herstellen kann. Diese Software ist so ausgebildet, dass getunnelte GPRS-Informationen aus- und eingepackt werden.

Beim Initialisieren der Verbindung wird überprüft, ob das mobile Endgerät Zugriff auf ein GPRS-Netzwerk haben darf, wobei bekannte Sicherheitsüberprüfungen basierend auf dem GPRS Modus stattfinden. Diese Authentifizierung wird ebenfalls durch Übertragung von getunnelten Informationen erreicht. Ein entsprechendes Modul, wie es weiter unten beschrieben wird ist Bestandteil der Software. Es ist jedoch auch denkbar, dass die Software in die bestehenden Authentifizierungsverfahren auf dem mobilen Endgeräten eingreift, sodass es keines separaten Moduls bedarf.

Zum Aufbau einer Verbindung wird vorzugsweise eine Broadcast-Nachricht gesendet, um einen IP Serving GPRS Support Node im IP-Netzwerk zu finden, durch den ein Tunnel aufgebaut wird.

In einer bevorzugten Ausführungsform kann weiterhin ein HLR-Dienst vorhanden sein, der sowohl auf der Grundlage der IP-Adresse des Endgerätes als auch auf anderen GPRS typischen Informationen (die auf dem mobilen Endgerät z. B. in Form einer Subscriber Identity Module –SIM- vorliegen) eine Authorisierung und/oder Lokalisierung des Endgerätes erlaubt. Ein solcher HLR-Dienst hat die Aufgabe festzustellen bzw. zu speichern, wo sich ein mobiles Endgerät befindet und wem dieses bzw. welcher Telefonnummer dieses zugeordnet ist. Außerdem vergibt der Netzwerkanbieter mittels des HLR Dienstes Benutzer- und/oder Geräte-spezifische Rechte, die aufgrund der Besonderheit dieses Verfahrens auch in nicht-GSM/UMTS Netzen genutzt werden kann.

Gerade bei mobilen Netzwerken ist es von Bedeutung, wie ein hand over zwischen den Basisstationen erfolgen kann. Ein solcher hand over erfolgt immer dann, wenn das mobile Endgerät aus dem Empfangsbereich einer Basisstation in den Empfangsbereich einer anderen Basisstation kommt. In der bevorzugten Ausführungsform kann ein hand over sowohl auf IP-Ebene als auch auf GPRS-Ebene erfolgen. Die Form des hand overs erfolgt in Abhängigkeit davon, in welchem Netzwerk sich das Endgerät befindet bzw. zwischen welchen Netzwerktypen gewechselt wird. Sollte das mobile Endgerät z. B. im Bereich eines Wireless-Netzwerk bleiben, so erfolgt der hand over vorzugsweise auf IP-Basis. Sollte hingegen ein Wechsel der Domänen erfolgen, so kann das hand over auf der Basis von GPRS erfolgen. Als Besonderheit nutzt diese Anwendung einen Mechanismus, der die zukünftige Entwicklung der Verbindungsqualität der verschiedenen Netzwerktypen voraussagt. Aufgrund dieser Voraussage wird das hand over von einem Netzwerktyp zum anderen zeitlich optimiert.

Bei mobilen und drahtlosen Kommunikationen ist es von Vorteil, wenn die Informationen verschlüsselt werden. In der bevorzugten Ausführungsform wird Ipsec auf IP-Ebene verwendet. Es ist jedoch auch denkbar andere Verschlüsselungsverfahren anzuwenden. Mehrere Verfahren können auch parallel eingesetzt werden.

Wie bereits oben ausgeführt wurde, ist neben dem Verfahren eine Vorrichtung Bestandteil der Erfindung, die im IP-Netzwerk angeordnet ist und dort die Funktion eines IP SGSN übernimmt. Hierbei handelt es sich um eine Vorrichtung zur Bereitstellung von GPRS Diensten in einem IP-Netzwerk, mit Mitteln die eine bekannte Funktionalität eines Serving GPRS Support Node in einem GPRS-und/oder UMTS-Netzwerk ermöglichen. Durch diese vollständige Kompatibilität zu bekannten SGSN bzw. GGSN (Gateway GSN) erfolgt eine Kommunikation mit bestehenden Netzwerken ohne großen technischen Aufwand. Die Besonderheit der Vorrichtung liegt jedoch darin, dass mit den vorzugsweise mobilen Endgeräten auf der Basis eines IP-Tunnels kommuniziert wird, wobei durch den IP-Tunnel GPRS-Pakete übertragen werden.

Wie bereits oben beschrieben wurde, kann der IP SGSN in jedem IP basierten Netzwerk eingesetzt werden. Er ist so ausgebildet, dass er Verbindungen zu SGSN's, GGSN's, HLR's, CGF's in das UMTS/GSM-Heimatnetzwerk aufbauen kann. Vom UMTS-Netzwerk gesehen, handelt es sich somit um einen normalen "3G"-SGSN, wie er in den 3GPP-Dokumenten spezifiziert wurde.

In Verbindung mit dem angepassten HLR-Service kann der IP SGSN unterschiedliche Dienste zu unterschiedlichen Servern routen. (z. B. Internet und E-mail zum "local" proxy- und Mail-server, oder andere GPRS services zu GGSN des UMTS/GSM-Providers).

Der spezifische HLR und CGF sind keine wesentlichen Bestandteile für "GPRS über ein IP basiertes Netzwerk". Sie ermöglichen vielmehr weitere Funktionalitäten, die der Netzwerkprovider seinen Kunden anbieten möchte.

Der angepasste HLR arbeitet wie ein bekannter transparenter HLR im IP basierten Netzwerk. Er besitzt eine Liste aller Halter, die ein Roaming ermöglichen. Hierbei handelt es sich um HLRs von UMTS/GSM-Providern, die ein Roamingabkommen miteinander abgeschlossen haben. Somit fragt der IP SGSN den angepassten HLR anstatt eines anderen. Der angepasste HLR entscheidet, ob das Paket vom IP SGSN zu einem HLR geschickt werden soll, und wenn ja zu welchem. Der Provider kann ebenfalls seine eigene subscriber list im angepassten HLR verwalten. Weiterhin kann der Provider in diesem HLR eine Liste verwalten, in dem die angebotenen Dienste, die dem Benutzer zur Verfügung stehen, abgespeichert sind.

Der angepasste CGF arbeitet ebenfalls transparent wie ein bekannter CGF jedoch im IP basierten Netzwerk. Hierdurch ist es möglich, Informationen zu sammeln, die eine Berechnung der Kosten bzw. Gebühren für den Benutzer ermöglichen. Anstatt einer Verbindung zu einem herkömmlichen CFG aufzubauen, baut der IP SGSN eine Verbindung zum angepassten CGF auf. Der so modifizierte CGF kann die Informationen weiterleiten an den Provider oder eigene Berechnungen vornehmen.

In einer bevorzugten Ausführungsform weist die Vorrichtung Mittel auf, die eine Gatewayfunktionalität bereitstellen, insbesondere das Routen von Informationen in andere Netzwerke. In diesem Fall handelt sich um ein IP-GGSN. Entsprechende Systeme sind aus den anderen Netzwerken bekannt.

Wie bereits oben ausgeführt wurde, kann die Vorrichtung ebenfalls die Funktionalität eines HLR übernehmen. Hierbei ist insbesondere zu erwähnen, dass Mittel vorhanden sind, die das Abbilden einer IP-Adresse in einem HLR erlauben. Weiterhin sind sowohl Mittel vorhanden, die ein hand over auf den unterschiedlichen Protokollebenen und Protokollen ermöglichen, sowie Mittel, die eine Verschlüsselung ermöglichen.

Weitere Bestandteile der Vorrichtung sind Mittel, die Broadcast-Nachrichten eines Endgerätes empfangen können, um hierdurch eine GPRS-Tunnelverbindung aufzubauen. Nach dem Empfang eines solchen Paketes wird eine Antwort an das mobile Endgerät gesendet, aus der das mobile Endgerät entnehmen kann, dass sich ein IP SGSN im Netzwerk befindet.

Ein weiterer Bestandteil der Erfindung ist ein Endgerät, das in der Lage ist, mit dem IP SGSN durch eine Tunnelverbindung zu kommunizieren. Herkömmliche Endgeräte, wie PDAs oder mobile Telefone, weisen solche Funktionalitäten jedoch nicht auf. Vielmehr bedarf es einer Anpassung der Software und ggf. der Hardware, um eine solche Kommunikation zu ermöglichen. Im Wesentlichen weisen diese modifizierten Endgeräte Mittel auf, die einen Austausch von Informationen über GPRS durch einen IP-Tunnel ermöglichen. Voraussetzung ist natürlich, dass ein entsprechender IP SGSN zur Kommunikation bereitsteht.

In einer bevorzugten Ausführungsform handelt es sich um ein Gerät, das mehrere Funkstandards unterstützt. So kann das Gerät vorzugsweise sowohl Wireless Lan als auch UMTS oder GSM/GPRS unterstützen.

Aufgrund des Einsatzes in IP-Netzwerken sollten bekannte Verfahren zur Adresskonvertierung implementiert sein. Dies erlaubt eine höhere Flexibilität beim Einsatz in Netzwerken, die z. B. unterschiedliche IP-Versionen unterstützen. So sollte Adresskonvertierung erlaubt sein, insbesondere von Ipv4 nach IPv6 und umgekehrt sowie NAT bzw. Maskieren von Adressen.

Weiterhin sind in der bevorzugten Ausführungsform Mittel vorhanden, die eine Verschlüsselung der Informationen erlauben. Möglichkeiten der Verschlüsselung wurden bereits oben diskutiert. Gerade bei der Initialisierung ist es wichtig, dass Mittel vorhanden sind, die eine Authentifizierung im GPRS-Netzwerk ermöglichen. Ein Zugriff

auf das HLR wird hierbei vorzugsweise vorgenommen. Durch diesen Ansatz ist es möglich, Kosten eindeutig zuzuordnen.

In der bevorzugten Ausführungsform ist ein Softwarelayer vorhanden, der die beschriebene Funktionalität ermöglicht, wobei dieser vorzugsweise einen Zugriff auf einen IP-Stack besitzt. Durch das Abgreifen bzw. Umleiten der Informationen im IP-Stack, der bei GPRS-bzw. UMTS-Endgeräten vorhanden ist, kann eine einfache Implementierung erfolgen.

Ein weiterer Bestandteil der Erfindung ist eine Software, die die beschriebene Funktionalität auf einem herkömmlichen Endgerät implementiert. Es sei darauf hingewiesen, dass sich der Schutz ebenfalls auf einen Datenträger mit einer solchen Software erstrecken soll.

Durch diesen Ansatz erreicht man, dass man neue Netzwerk Arten einfach in bestehende Netze integriert. Die Funktionalität der bekannten Netzwerke kann weiterhin genutzt werden, wobei auf neue Technologien zurückgegriffen werden kann, die durch die neuen Netzwerken bereitgestellt werden.

Im Folgenden wird die Erfindung anhand von Ausführungsbeispielen näher erläutert, die in den Figuren schematisch dargestellt sind. Gleiche Bezugsziffern in den einzelnen Figuren bezeichnen dabei gleiche Elemente. Im Einzelnen zeigt:

Fig. 1 ein mobiles Endgerät, das 3 Bänder unterstützt, nämlich UMTS, GSM und WLAN, die jeweils in unterschiedlichen Domänen verwendet werden, wobei das mobile Endgerät über Basisstationen mit SGSN verbunden ist, die über GGSN wiederum die Verbindung zu unterschiedlichen Domänen herstellen;

Fig. 2 eine Hierarchie beginnend mit Endgeräten (UE) über Basisstationen (UTRAN), (Serving) Radio-Network Controller, SGSN, GGSN, sowie HLR

Fig. 3 eine logische Architektur eines (UMTS) GPRS-Netzwerkes;

Fig. 4 Anwenderebenen für GPRS über GSM;

Fig. 5 Anwenderebenen für GPRS über UMTS;

Fig. 6 Anwenderebenen für GPRS über IP;

Fig. 7 Kontrollebenen für GPRS über GSM;

Fig. 8 Kontrollebenen für GPRS über UMTS;

Fig. 9 Kontrollebenen für GPRS über IP;

Fig. 10 Struktur des Softwaremoduls, das auf einem mobilen Endgerät angeordnet ist.

Fig. 1 zeigt ein mobiles Endgerät, das 3 Bänder unterstützt, nämlich UMTS, GSM und WLAN, die jeweils in unterschiedlichen Domänen verwendet werden. Das mobile Endgerät bewegt sich durch die Netzwerke, wobei ein Roaming über GPRS stattfindet. Um dies zu gewährleisten, müssen entsprechende Gateways (GGSN) eingesetzt werden, die die Verbindung zwischen den Netzwerken herstellen. Im Netzwerk, in dem das WLAN eingesetzt wird, kommt das erfindungsgemäße IP SGSN (fm SGSN) zum Einsatz, das über einen IP-Tunnel mit dem Endgerät kommuniziert. Für die weitere Kommunikation werden die Informationen über die SGSN und GGSN transportiert.

Fig. 2 zeigt eine Hierarchie, wie sie in bekannten (UMTS) Netzwerken anzutreffen ist. Details hierzu können in der Literatur [13] gefunden werden. Die Hierarchie beginnt mit

einem Endgerät (UE), das per Funk über Basisstationen (UTRAN), über einen Serving) Radio-Network Controller (SRNC) mit SGSN, GGSN verbunden ist. Die SGSN und GGSN haben Zugriff auf das HLR. Der Radio Network Controller hat die Aufgabe, die Bandbreite und Frequenzen bzw. Timeslots zu verteilen.

Die Figur 3 zeigt eine logische Architektur eines GPRS-Netzwerkes, wie es aus [13] bekannt ist. Hieraus ist ersichtlich, dass das Netzwerk im Wesentlichen aus den SGSN und den GGSN aufgebaut ist, die einerseits die Verbindung der mobilen Endgeräte in den Domänen kontrollieren und andererseits die Verbindung zu anderen Netzwerken ermöglichen. In einem Netzwerk können mehrere GGSN vorhanden sein, die miteinander verbunden sind. Die SMS-GMSC und SMS-IWMSC sind Einheiten, die für den SMS-Austausch eingesetzt werden. Weitere Details können [13] entnommen werden.

Die Figuren 4, 5 und 6 zeigen die Benutzerebenen des bekannten GPRS über GSM/UMTS-Protokolls und des über IP getunnelten GPRS-Protokolls. In diesem Zusammenhang wird auf die Literatur [13] verwiesen. Es wird deutlich, dass das getunnelte Protokoll GTP-U in Figur 6. sowohl zwischen dem GGSN als auch zwischen dem Endgerät verwendet wird. Dies dient dazu, die IP-Pakete zu transportieren. Es wird lediglich das GTP-U-Protokoll auf einer UDP/IP-Schicht verwendet. Im Gegensatz zu UMTS bedarf es keiner Basisstationen, die zusätzlich über das Packet Data Convergence Protocol mit dem Endgerät kommuniziert. Es ist somit ein direkter Tunnel zum Endgerät gegeben. Für weitere Details wird auf die Literatur [20] verwiesen.

Die Figuren 7 , 8 und 9 zeigen die Unterschiede auf der Kontrollebene.

Als weitere Ebene wird Radio Access Network Application Protocoll (RANAP) eingesetzt, wie es in [20] beschrieben wurde. Dieses Protokoll kapselt und transportiert

Informationen und Signale auf höheren Ebenen. Die Ebenen unterhalb von RANAP werden in [14] beschrieben. Für den Transport von RANAP-Informationen sollte SCCP eingesetzt werden. Dies sollte konform sein mit dem ITU-T white book.

Die vorliegende Erfindung basiert im Wesentlichen auf einem Server und einem Client. Sowohl der Client als auch das Server müssen GPRS über IP unterstützen.

Die Module des Clients unterstützen eine Reihe von neuen Standards wie (3GPP specs, IETF RFC's) oder Entwürfe (Drafts), die nicht Teil des IP-Stacks sind, sondern auf ihm aufbauen. Der modulare Ansatz hat den Vorteil, dass eine einfache Anpassung möglich ist.

Die Struktur des Clients kann der Figur 10 entnommen werden.

Der Authenticator ist verantwortlich für das Management von unterschiedlichen Informationen wie Passwörtern, öffentlichen und privaten Schlüsseln, Zertifikaten und USIM. Er umfasst ebenfalls Verfahren zur Authentifizierung. Für GPRS über IP basierte Netzwerke ist die Authentifizierung gemäß den GSM- und UMTS-Standards, wie sie in [10] und [25] offenbart werden, notwendig.

Der Sicherheitsagent ist verantwortlich für die Sicherheit und Integrität der Verbindung. Er verwendet Verschlüsselungsmethoden und paketbasierte Filter und Firewall-Mechanismen. Für GPRS über IP basierte Netzwerke sollte IPSec mit IKE (Internet Key Exchange, [28]) unterstützt werden.

Neben den beiden Modulen gibt es weitere Module nämlich den Tunnel-Manager und den Adresskonverter.

Der Tunnelmanager ist verantwortlich für das Tunnelmanagement und das Handover von Tunnelendpunkten. Für GPRS über IP basierte Netzwerke sollte GTP ([22]) unterstützt werden.

Der Adressenkonverter hat die Aufgabe der Adresskonvertierung, in der Regel von Ipv4 zu Ipv6 ([30]) und umgekehrt. Dies ist deswegen notwendig, weil die Stacks der Endgeräte nur die Version 4 unterstützen. Ältere Netzwerke sind ebenfalls auf die älteren Versionen ausgerichtet. Hingegen werden neuere Netzwerke, wie UMTS, auf den neueren Versionen basieren. Insbesondere dann, wenn hand over zwischen den unterschiedlichen Netzwerken erfolgt, ist eine Konvertierung notwendig. Die Unterstützung der Maskierung bzw. Adressenübersetzung ist ebenfalls von Interesse ([29]).

Liste der Literatur:

[1] GSM 01.61, General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements
[2] GSM 03.40, Technical Realization of the Short Message Service (SMS) Point-to-poin (PP)
[3] GSM 04.08, Mobile radio interface layer 3 specification
[4] GSM 04.60, General Packet Radio Service (GPRS); Mobile Station (MS) - Base Station System (BSS) interface; Radio Link Control/ Medium Access Control (RLC/MAC) protocol
[5] GSM 04.64, General Packet Radio Service (GPRS); Mobile Station - Serving GPRS Support Node (MS-SGSN) Logical Link Control (LLC) layer specification
[6] GSM 04.65, General Packet Radio Service (GPRS); Mobile Station (MS) - Serving GPRS Support Node (SGSN); Subnetwork Dependent Convergence Protocol (SNDCP)
[7] GSM 08.16, General Packet Radio Service (GPRS); Base Station System (BSS) - Serving GPRS Support Node (SGSN) Interface; Network Service
[8] GSM 08.18, General Packet Radio Service (GPRS); Base Station System (BSS) - Serving GPRS Support Node (SGSN); BSS GPRS Protocol
[9] GSM 09.02, Mobile Application Part (MAP) Specification
[10] 3GPP TS 23.003 v5.1.0, Numbering, Addressing and Identification
[11] 3GPP TS 23.015 v4.0.0, Technical realization of Operator Determined Barring (ODB)
[12] 3GPP TS 23.040 v5.1.0, Technical realization of Short Message Service (SMS)
[13] 3GPP TS 23.060 v4.2.0, General Packet Radio Service (GPRS) Service description; Stage 2
[14] 3GPP TS 23.121 v3.5.1, Architecture Requirements for release 99
[15] 3GPP TS 24.008 v5.1.0, Mobile radio interface Layer 3 specification; Core network protocols; Stage 3
[16] 3GPP TS 25.301 v4.1.0, Radio Interface Protocol Architecture
[17] 3GPP TS 25.321 v4.2.0, Medium Access Control (MAC) protocol specification
[18] 3GPP TS 25.322 v4.2.0, Radio Link Control (RLC) protocol specification
[19] 3GPP TS 25.323 v4.2.0, Packet Data Convergence Protocol (PDCP) specification
[20] 3GPP TS 25.413 v4.2.0, UTRAN Iu interface RANAP signalling
[21] 3GPP TS 29.002 v4.5.0, Mobile Application Part (MAP) specification
[22] 3GPP TS 29.060 v4.2.0, General Packet Radio Service

(GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface
[23] 3GPP TS 29.061 v4.2.0, Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based services and Packet Data Networks (PDN
[24] 3GPP TS 32.215 v4.0.0, Telecom Management; Charging management; Charging data description for the Packet Switched (PS) domain
[25] 3GPP TS 33.102 v4.2.0, 3G security; Security architecture
[26] RFC 2002, IP Mobility Support
[27] RFC 2284, PPP Extensible Authentication Protocol (EAP)
[28] RFC 2409, The Internet Key Exchange (IKE)
[29] RFC 3022, Traditional IP Network Address Translator
[30] RFC 3089, A SOCKS-based IPv6/IPv4 Gateway Mechanism

Patentansprüche

1. Verfahren zur Übertragung von Informationen mittels GPRS in einem IP-Netzwerk, insbesondere einem Wireless LAN und/oder einem Hiperlan Netzwerk, mit einem vorzugsweise mobilen Endgerät, das mit dem IP-Netzwerk in Verbindung steht, so dass IP-Pakete ausgetauscht werden können, mit einem IP Serving GPRS Support Node im IP-Netzwerk,
   - wobei beim Initialisieren der Verbindung zwischen dem Endgerät und dem IP Serving GPRS Support Node ein Tunnel auf der Basis von IP-Paketen aufgebaut wird, der GPRS-Informationen tunnelt,
   - wobei die Übertragung von Informationen durch den Tunnel erfolgt,
   - wobei der IP Serving GPRS Support Node über ein Netzwerk mit weiteren Serving GPRS Support Nodes verbunden ist, und die Informationen je nach Richtung der Kommunikation auspackt und/oder umpackt, um die Informationen den weiteren Serving GPRS Support Nodes zu senden, oder einpackt um die Informationen durch den Tunnel zum Endgerät zu senden.

2. Verfahren nach dem vorhergehenden Verfahrensanspruch, dadurch gekennzeichnet, dass auf dem mobilen Endgerät eine Software installiert ist, die getunnelte GPRS-Informationen auspackt.

3. Verfahren nach dem vorhergehenden Verfahrensanspruch, dadurch gekennzeichnet, dass beim Initialisieren der Verbindung überprüft wird, ob das mobile Endgerät Zugriff auf ein GPRS-Netzwerk haben darf, wobei bekannte Sicherheitsüberprüfungen basierend auf dem GPRS-Modus stattfinden.

4. Verfahren nach dem vorhergehenden Verfahrensanspruch, dadurch gekennzeichnet, dass durch Broadcast-Nachrichten ein IP Serving GPRS Support Node im IP-Netzwerk gesucht wird, um einen Tunnel aufzubauen.

5. Verfahren nach einem oder mehreren der vorhergehenden Verfahrensansprüche, dadurch gekennzeichnet, dass ein HLR-Dienst vorhanden ist, der sowohl auf der Grundlage der IP-Adresse des Endgerätes als auch auf den Adressinformationen von GPRS eine Bestimmung und/oder Lokalisierung des Endgerätes erlaubt

6. Verfahren nach einem oder mehreren der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass ein hand over sowohl auf IP-Ebene als auch auf GPRS-Ebene erfolgen kann, in Abhängigkeit davon, in welchem Netzwerk sich das Endgerät befindet.

7. Verfahren nach einem oder mehreren der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass eine Verschlüsselung auf GPRS- und/oder IP-Ebene, vorzugsweise durch ipsec, erfolgt.

8. Vorrichtung zur Bereitstellung von GPRS-Diensten in einem IP-Netzwerk, mit Mitteln, die eine Funktionalität eines Serving GPRS Support Node in einem GPRS und/oder UMTS ermöglichen, dadurch gekennzeichnet, dass Mittel vorhanden sind, die eine Kommunikation über GPRS durch einen IP-Tunnel mit einem Endgerät erlauben.

9. Vorrichtung nach dem vorherigen Vorrichtungsanspruch, dadurch gekennzeichnet, dass Mittel vorhanden sind, die eine Gatewayfunktionalität erlauben, insbesondere das Routen von Informationen in andere Netzwerke.

10. Vorrichtung nach einem oder mehreren der vorherigen Vorrichtungsansprüche, dadurch gekennzeichnet, dass

Mittel vorhanden sind, die das Abbilden einer IP-Adresse in einem HLR erlauben.

11. Vorrichtung nach einem oder mehreren der vorherigen Vorrichtungsansprüche, dadurch gekennzeichnet, dass Mittel vorhanden sind, durch die ein hand over sowohl auf IP-Ebene als auch auf GPRS-Ebene erfolgen kann, in Abhängigkeit davon, in welchem Netzwerk sich das Endgerät befindet .

12. Vorrichtung nach einem oder mehreren der vorhergehenden Vorrichtungsansprüche, dadurch gekennzeichnet, dass Mittel vorhanden sind, die eine Verschlüsselung auf GPRS- und/oder IP-Ebene, vorzugsweise durch ipsec, ermöglichen.

13. Vorrichtung nach einem oder mehreren der vorhergehenden Vorrichtungsansprüche, dadurch gekennzeichnet, dass Mittel vorhanden sind, die Broadcast-Nachrichten eines Endgerätes empfangen können, um hierdurch eine GPRS-Tunnelverbindung aufzubauen.

14. Endgerät mit Mitteln zur Kommunikation in einen IP-Netzwerk, insbesondere ein mobiles Endgerät, gekennzeichnet durch Mittel, die einen Austausch von Informationen über GPRS durch einen IP-Tunnel ermöglichen.

15. Endgerät nach dem vorherigen Endgeräteanspruch, dadurch gekennzeichnet, dass das Endgerät sowohl Wireless Lan als auch UMTS und/oder GSM unterstützt.

16. Endgerät nach einem oder mehreren der vorherigen Endgeräteansprüche, dadurch gekennzeichnet, dass Mittel vorhanden sind, die eine Adresskonvertierung erlauben, insbesondere von Ipv4 nach IPv6 und umgekehrt sowie NAT und/oder Maskieren.

17. Endgerät nach einem oder mehreren der vorherigen Endgeräteansprüche, dadurch gekennzeichnet, dass Mittel vorhanden sind, die eine Verschlüsselung der getunnelten Informationen ermöglichen bzw. die Tunnelpakete selber verschlüsseln, wobei vorzugsweise Ipsec eingesetzt wird.

18. Endgerät nach einem oder mehreren der vorherigen Endgeräteansprüche, dadurch gekennzeichnet, dass Mittel vorhanden sind, die eine Authentifizierung im GPRS-Netzwerk ermöglichen.

19. Endgerät nach einem oder mehreren der vorherigen Geräteansprüche, dadurch gekennzeichnet, dass ein Softwarelayer vorhanden ist, der die beschriebene Funktionalität ermöglicht, wobei dieser vorzugsweise einen Zugriff auf eine IP-Stack besitzt.

20. Software für Endgerät in einem IP Netzwerk, insbesondere ein mobiles Endgerät wie PDA oder ein mobiles Telefon, dadurch gekennzeichnet, dass ein Prozess implementiert wird, der einen Austausch von Informationen über GPRS durch einen IP-Tunnel ermöglicht.

21. Datenträger mit einer Datenstruktur, die in ein Endgerät geladen werden kann, wobei die Datenstruktur die Software nach dem vorhergehenden Anspruch umfasst.

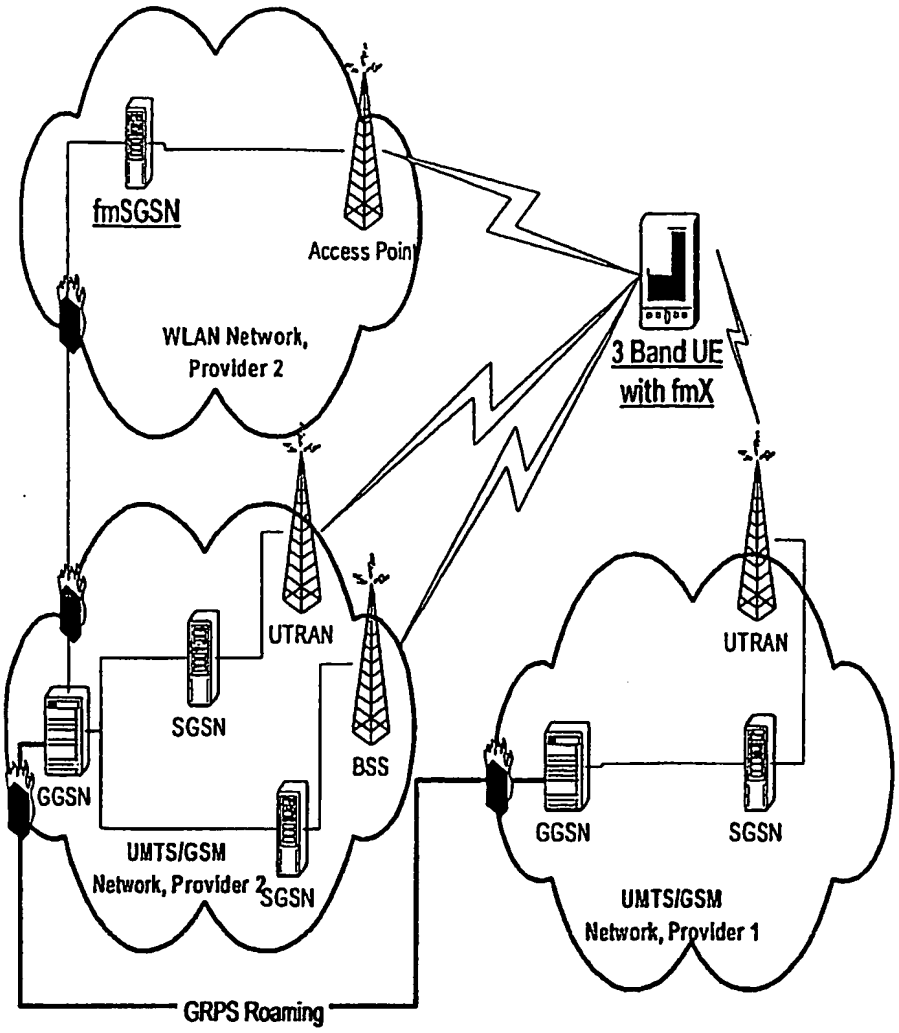
fmSGSN
Access Point
WLAN Network,
Provider 2
3 Band UE
with fmX
UTRAN
SGSN
BSS
GGSN
UMTS/GSM
Network, Provider 2
SGSN
UTRAN
GGSN
SGSN
UMTS/GSM
Network, Provider 1
GRPS Roaming

Fig. 1

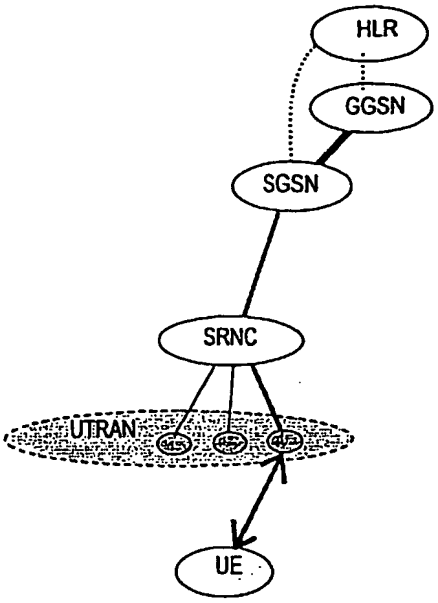
HLR
GGSN
SGSN
SRNC
UTRAN
UE

Fig. 2

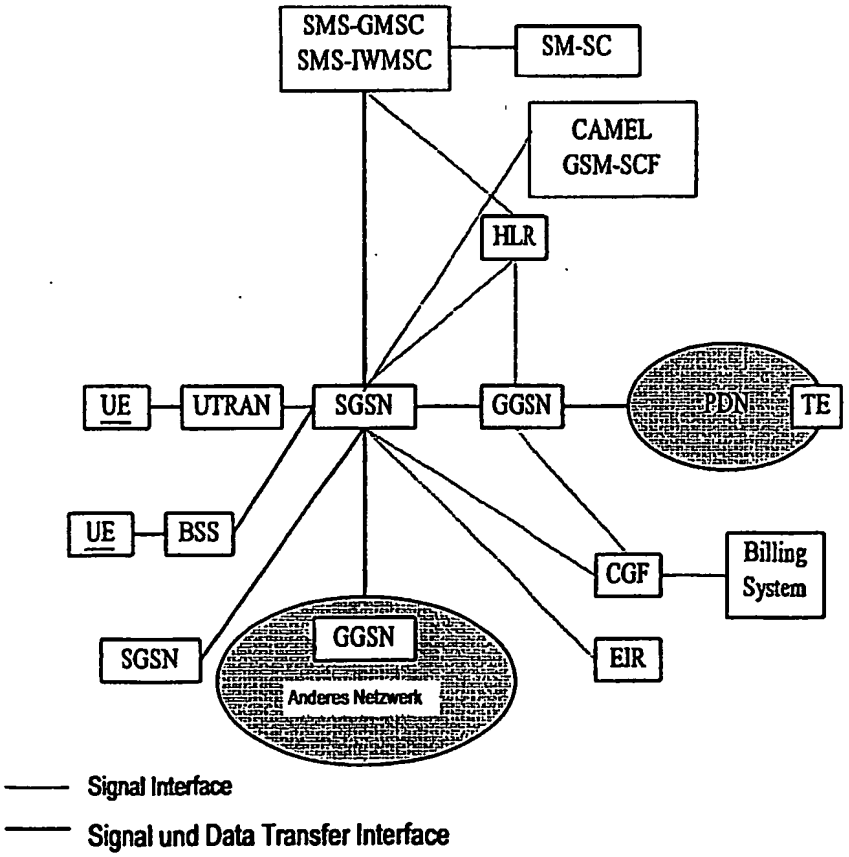
SMS-GMSC
SMS-IWMSC
SM-SC
CAMEL
GSM-SCF
HLR
UE
UTRAN
SGSN
GGSN
PDN
TE
UE
BSS
CGF
Billing
System
SGSN
GGSN
Anderes Netzwerk
EIR
Signal Interface
Signal und Data Transfer Interface

Fig. 3

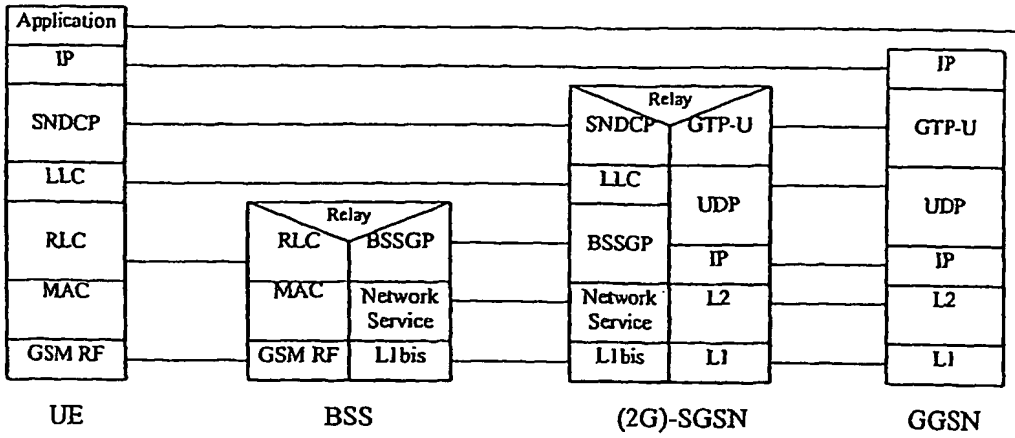

Fig. 4

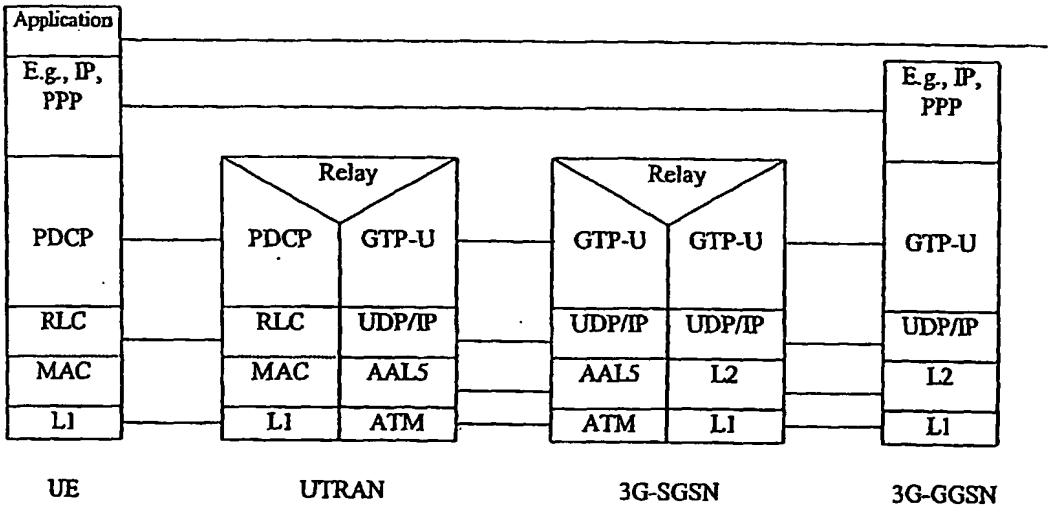

Fig. 5

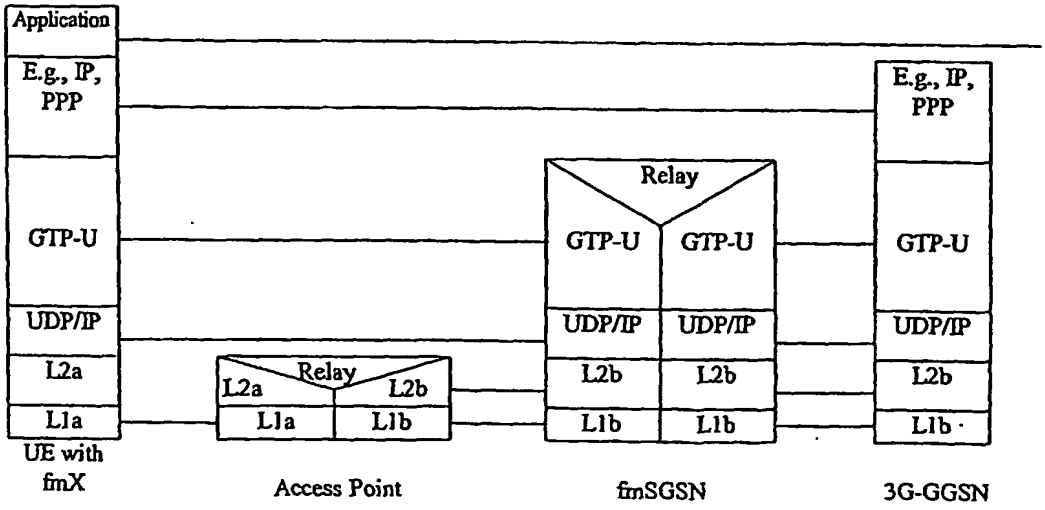

Fig. 6

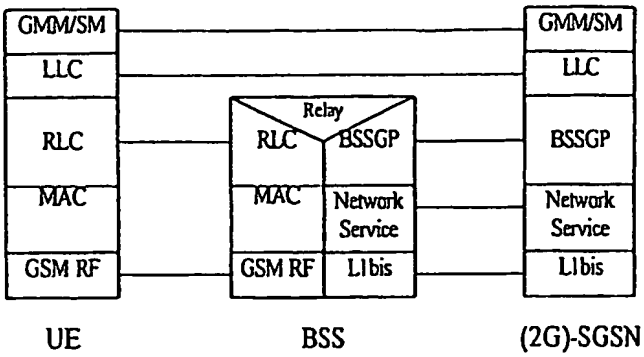

Fig. 7

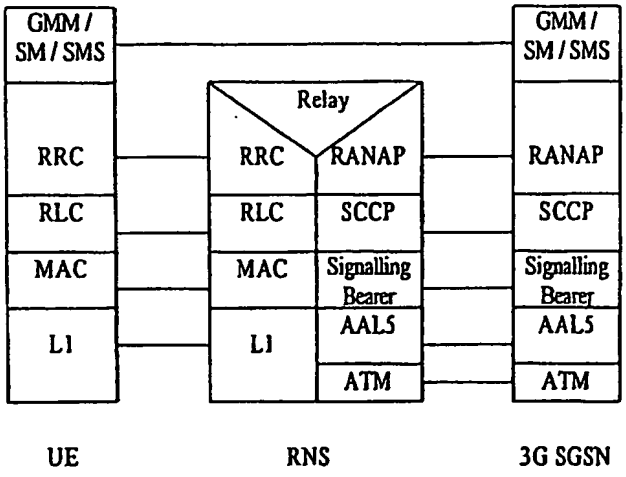

Fig. 8

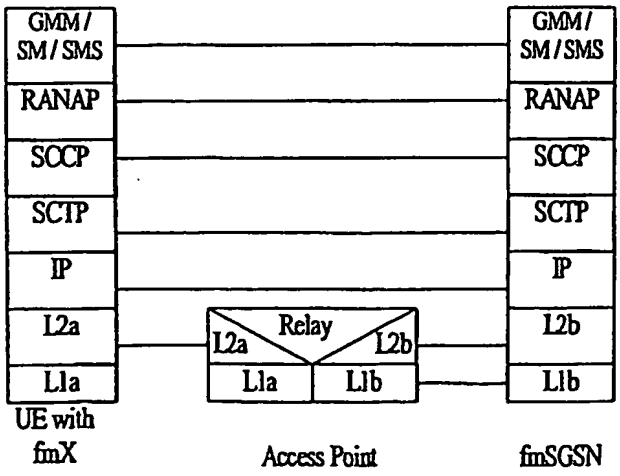

Fig. 9

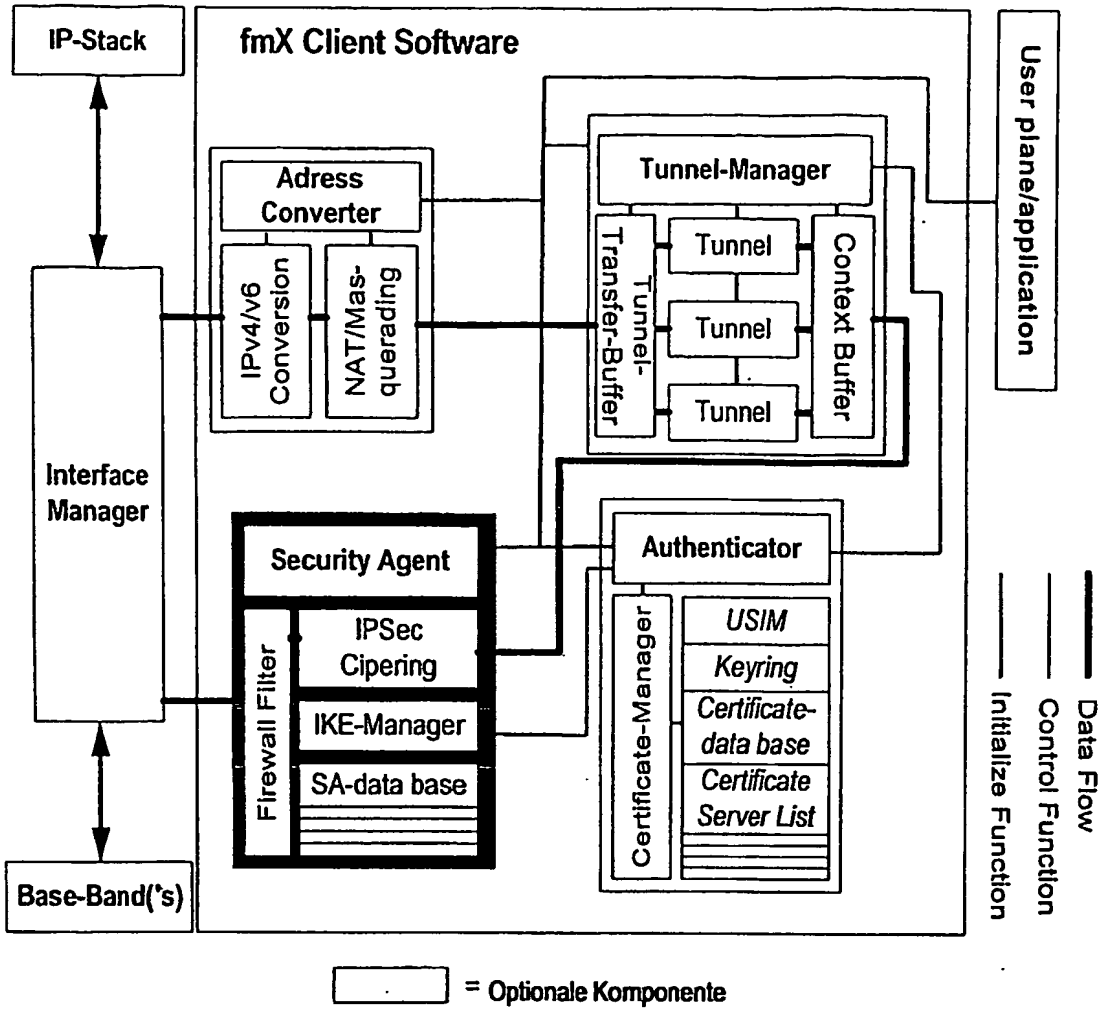
IP-Stack
fmX Client Software
User plane/application
Adress Converter
IPv4/v6 Conversion
NAT/Mas-quearding
Tunnel-Manager
Tunnel-Transfer-Buffer
Tunnel
Tunnel
Tunnel
Context Buffer
Interface Manager
Security Agent
Firewall Filter
IPSec Cipering
IKE-Manager
SA-data base
Authenticator
Certificate-Manager
USIM
Keyring
Certificate-data base
Certificate Server List
Base-Band('s)
Data Flow
Control Function
Initialize Function
= Optionale Komponente

Fig. 10